numero			Bellinzona
11	cl	0	7 gennaio 2020

Repubblica e Cantone Ticino
Consiglio di Stato
Piazza Governo 6
Casella postale 2170
6501 Bellinzona
telefono +41 91 814 43 20
fax +41 91 814 44 35
e-mail can-sc@ti.ch

Repubblica e Cantone Ticino

Il Consiglio di Stato

Dipartimento federale di giustizia e polizia
DFGP
Palazzo federale ovest
3003 Berna

anticipata per email: simone.rusterholz@fedpol.admin.ch, anna.wolff@fedpol.admin.ch, sandrine.favre@sem.admin.ch, helena.schaer@sem.admin.ch

Procedura di consultazione concernente il recepimento e trasposizione nel diritto svizzero delle basi legali concernenti la realizzazione dell'interoperabilità tra i sistemi d'informazione dell'UE nel settore delle frontiere, della migrazione e della polizia (regolamenti [UE] 2019/817 e [UE] 20189/818 (Sviluppi dell'acquis di Schengen)

Gentili signore,
Egregi signori,

abbiamo ricevuto la vostra lettera del 9 ottobre 2019 in merito alla summenzionata procedura di consultazione. L'avamprogetto del decreto federale, unitamente al relativo rapporto esplicativo sul recepimento e la trasposizione nel diritto svizzero delle basi legali concernenti la realizzazione dell'interoperabilità tra i sistemi d'informazione dell'UE nel settore delle frontiere, della migrazione e della polizia, è stato da noi esaminato in collaborazione con i servizi di polizia interessati e l'Ufficio cantonale della migrazione.

Nella fase di allestimento della risposta è stato consultato anche l'Incaricato cantonale per la protezione dei dati, che ha formulato osservazioni che divergono da quelle presentate in questo scritto. Ci permettiamo pertanto di allegare alla presente la sua presa di posizione del 12 dicembre 2019.

Ringraziando per l'opportunità che ci viene offerta di esprimere il nostro giudizio, formuliamo le seguenti osservazioni.

1. Considerazioni generali

In generale, l'Esecutivo cantonale accoglie favorevolmente la realizzazione dell'interoperabilità tra i vari sistemi d'informazione UE ritenuto che tale principio di interconnessione dei sistemi d'informazione centrali non può che portare indubbi vantaggi anche agli Uffici cantonali della migrazione e alle Polizie cantonali. Infatti essa permette la condivisione tempestiva e completa delle informazioni rilevanti atte alle gestioni della migrazione e alla prevenzione della migrazione irregolare, così da poter comparare in maniera intelligente ed efficiente una serie d'informazioni

utili all'attività corrente. Ad esempio è indubbia l'utilità del rilevatore delle identità multiple (MID) per scovare se una persona tenta di ottenere un permesso o un visto d'entrata, per accedere sul nostro territorio sotto false generalità, grazie alla comparazione di dati presenti nei diversi sistemi d'informazione UE. In precedenza ciò non era possibile poiché tra questi sistemi non vi era scambio d'informazioni e ciò permetteva ai malintenzionati di accedere illecitamente con un'identità di un'altra persona allo Spazio Schengen sfruttando queste lacune.

Anche per quel che concerne l'ambito di polizia, le modifiche proposte non possono che venire accolte positivamente, in quanto le stesse permettono di prevenire in modo più efficiente la violenza, la criminalità e il terrorismo e di combatterli efficacemente, colmando le attuali lacune in materia di sicurezza e consentendo l'esecuzione di controlli più efficaci alle frontiere esterne.

2. Considerazioni sugli articoli delle Leggi oggetto di modifica

2.1 Legge federale del 16 dicembre 2005 sugli stranieri e la loro integrazione (LStrI)

Ad art. 110c cpv. 1 lett. c (Consultazione del CIR a fini di individuazione di identità multiple)

Accogliamo favorevolmente il fatto che i Servizi cantonali della migrazione competenti in materia di visti siano contemplati tra le Autorità che possono accedere ai dati e ai riferimenti conservati nel Registro delle identità comuni (CIR), banca dati comune che raccoglie i dati inerenti all'identità dei cittadini di Stati terzi, al fine di individuare le identità multiple. Ciò contribuirà in maniera efficace e tempestiva ad evitare abusi nell'ambito del rilascio dei visti, a persone che richiedono il visto con una falsa identità con secondi fini, quali quello di giungere nel nostro Paese per compiere atti illeciti oppure per raggirare un divieto d'entrata in corso di validità.

Ad art. 120d (trattamento indebito di dati personali nei sistemi d'informazione)

Per quanto attiene alla punibilità dei funzionari con una multa fino a CHF 10'000.--, in caso di trattamento indebito dei dati personali presenti nei sistemi d'informazione UE (ORBIS, C-VIS, EES, ETIAS e CIR), non abbiamo nulla da osservare ritenuto che si tratta di un'estensione ai fini dell'interoperabilità.

2.2 Legge federale del 20 giugno 2003 sul sistema d'informazione per il settore degli stranieri e dell'asilo (LSISA)

A tal proposito, lo scrivente Esecutivo cantonale saluta positivamente le modifiche e non ha particolari osservazioni da formulare.

2.3 Legge del 14 marzo 1958 sulla responsabilità

Considerato come questo dispositivo di legge trovi applicazione unicamente per persone cui è conferita una carica pubblica della Confederazione, lo scrivente Consiglio non ha osservazioni da formulare in proposito.

2.4 Legge federale del 13 giugno 2008 sui sistemi d'informazione di polizia della Confederazione

Come indicato in entrata, l'Autorità di polizia accoglie favorevolmente l'interoperabilità tra i sistemi d'informazione. Tale principio permette infatti di migliorare la celerità e la qualità della consultazione delle banche dati, agevolendo non solo lo snellimento della procedura soprattutto ai servizi di polizia che sono tenuti a consultare le stesse diverse volte al giorno alfine di rispondere alle richieste dei colleghi della Confederazione e delle Autorità estere, ma altresì adattamenti necessari alfine di combattere efficacemente la criminalità internazionale di ogni tipo.

Si ritiene inoltre fondamentale il collegamento tra la Polizia cantonale e le Autorità preposte della migrazione, considerato come quest'ultima funga spesso da vettore di individui legati al terrorismo, in particolare di matrice islamica.

3. Conclusioni

Si rinnovano i ringraziamenti per averci dato la possibilità di prendere posizione nell'ambito della procedura in consultazione in parola.

Dal lato finanziario rileviamo che i Cantoni non dovrebbero venir toccati in maniera rilevante poiché il grosso dei costi informatici e di gestione sarà a carico dell'Ufficio federale di polizia (fedpol) e della Segreteria di Stato della migrazione (SEM). I costi dei Cantoni saranno limitati alle modifiche informatiche per aggiornare i vari applicativi che consentono l'accesso alle menzionate banche dati UE. Il collegamento dei sistemi svizzeri al portale di ricerca ESP richiederà ad esempio modifiche tecniche dei sistemi cantonali d'interrogazione. Dal rapporto esplicativo i costi a carico dei Cantoni al momento attuale non sono ancora quantificabili. Non è infatti ancora possibile valutare in quale misura i Cantoni saranno coinvolti, ad esempio nelle verifiche operate mediante il rilevatore delle identità multiple (MID), ritenuto che i processi concreti per la verifica dei collegamenti di questa componente centrale devono ancora essere definiti (cfr. pto. 6.3 rapporto esplicativo, pag. 60).

In questo contesto di incertezza circa l'impatto finanziario e i possibili oneri supplementari, benché compensati dai vantaggi l'introduzione del concetto di interoperabilità comporterà, lo scrivente Consiglio di Stato non può nascondere delle legittime preoccupazioni. Sarebbe infatti auspicabile una maggiore chiarezza e trasparenza in questo ambito da parte delle Autorità federali, in modo tale che i Cantoni abbiano concretamente la possibilità di valutare la portata di un simile progetto in termini economici e anche organizzativi. Ciò che attualmente non ci è possibile.

Vogliate gradire, gentili Signore ed egregi Signori, l'espressione della nostra stima.

PER IL CONSIGLIO DI STATO

Il Presidente:

Christian Vitta

Il Cancelliere:

Arnoldo Coduri

Allegato:
- Osservazioni del 12 dicembre 2019 dell'Incaricato cantonale della protezione dei dati.

Copia per conoscenza a:
- Dipartimento delle istituzioni (di-dir@ti.ch);
- Segreteria generale del Dipartimento delle istituzioni (di-sg.ap@ti.ch);
- Sezione della popolazione (di-sp.direzione@ti.ch);
- Comando della Polizia cantonale (servizio.giuridico@polca.ti.ch);
- Deputazione ticinese alle Camere federali (can-relazioniesterne@ti.ch);
- Pubblicazione in Internet.

Via Canonico Ghiringhelli 1
6501 Bellinzona

telefono +41 91 814 45 01
web www.ti.ch/protezionedati

Repubblica e Cantone Ticino
Cancelleria dello Stato
Servizi giuridici del Consiglio di Stato

persona incaricata Akou Carine Anato

Incaricato cantonale della protezione dei dati
6501 Bellinzona

telefono +41 91 814 45 03
e-mail carine.anato@ti.ch

Polizia Cantonale
Servizi generali
Servizio giuridico
Via Chicherio 20
6501 Bellinzona

Bellinzona 12 dicembre 2019

Ns. riferimento 2019.286

Procedura di consultazione – Decreto federale che approva e traspone i regolamenti (UE) 2019/817 e 2019/818 sull'interoperabilità (sviluppi dell'acquis di Schengen)

Gentile signora Rüegsegger, cara Bernadette,

le trasmettiamo il parere dell'Incaricato cantonale della protezione dei dati personali in merito al recepimento e la trasposizione nel diritto svizzero delle basi legali concernenti la realizzazione dell'interoperabilità tra i sistemi di informazione dell'UE nel settore delle frontiere, della migrazione e della polizia (regolamenti UE 2019/817 E 2019/818).

Introduzione

I regolamenti in questione mirano in linea generale a migliorare la gestione delle frontiere esterne dello spazio Schengen e a contribuire alla sicurezza interna dell'Unione europea. A tal fine, istituiscono un quadro per garantire l'interoperabilità tra i sistemi di informazione su larga scala dell'UE esistenti e futuri nei settori dei controlli alle frontiere, dell'asilo e dell'immigrazione, della cooperazione giudiziaria e di polizia in materia penale. I due regolamenti 2019/817 e 2019/818 costituiscono degli acquis di Schengen in materia di frontiere e visti (vale a dire il VIS, l'EES, il sistema ETIAS e il SIS) e in materia di cooperazione di polizia (il sistema Eurodac, il sistema ECRIS-TCN e il SIS).

Le componenti dell'interoperabilità istituite dai regolamenti riguardano tre sistemi d'informazione già esistenti, ossia il sistema d'informazione Schengen (SIS), il sistema Eurodac e il sistema di informazione visti (VIS); tre sistemi ancora in preparazione o

sviluppo, il sistema di ingressi/uscite (EES, *Entry-Exit System*), il sistema europeo di informazione e autorizzazione ai viaggi (ETIAS) e il sistema europeo di informazione sui casellari giudiziali riguardo ai cittadini di paesi terzi (sistema ECRIS-TCN); la banca dati Interpol sui documenti di viaggio rubati o smarriti (SLTD) e i dati Europol.

Contenuto dei principali sistemi informatici da interconnettere

I tre sistemi d'informazione già esistenti sono complementari e, ad eccezione del SIS, riguardano essenzialmente i cittadini di paesi terzi. Essi servono principalmente alla gestione delle frontiere, ad eccezione del SIS che ha anche accessoriamente delle funzioni di contrasto della criminalità.

Il SIS è la più grande e più diffusa piattaforma di scambio di informazioni sull'immigrazione e il contrasto della criminalità. Esso è consultato dalle autorità di polizia, di controllo delle frontiere e della immigrazione. Contiene le cartelle dei cittadini di paesi terzi cui è fatto divieto di entrare o di soggiornare nello spazio Schengen, dei cittadini dell'UE e di paesi terzi che sono scomparsi o ricercati (minori compresi) e degli oggetti ricercati (armi da fuoco, veicoli, documenti d'identità, attrezzature industriali, ecc.).

Il sistema europeo di dattiloscopia, EURODAC, contiene le impronte digitali dei richiedenti asilo e dei cittadini di paesi terzi che attraversano irregolarmente le frontiere esterne di Schengen.

Il VIS è un sistema centralizzato per lo scambio di dati tra Stati membri sui visti per soggiorni di breve durata. Elabora i dati e le decisioni inerenti alle domande di visto per soggiorni di breve durata, a fini di visita o di transito attraverso l'area Schengen.

L'EES (Entry-Exit System) è un sistema centralizzato di gestione delle frontiere, anch'esso riguardante i cittadini di paesi terzi.

L'ECRIS è un sistema elettronico per lo scambio di informazioni sulle condanne pronunciate a carico di una determinata persona dagli organi giurisdizionali penali all'interno dell'UE. I sistemi ECRIS e Europol sono principalmente dei sistemi di contrasto della criminalità.

Modalità dell'interoperabilità

L'interoperabilità tra tali sistemi avrà quattro componenti ossia, un portale di ricerca europeo («ESP»), un servizio comune di confronto biometrico («BMS comune»), un archivio comune di dati di identità («CIR») e un rilevatore di identità multiple («MID»).

L'ESP ha lo scopo di offrire un'interfaccia semplificata che fornisca risultati dell'interrogazione rapidi in modo trasparente. Ciò permetterebbe l'interrogazione simultanea dei diversi sistemi sulla base dei dati di identità (sia anagrafici sia biometrici). In altre parole, l'utente finale potrebbe effettuare un'unica ricerca e ottenere risultati da tutti i sistemi cui è autorizzato ad accedere invece di interrogare ogni sistema singolarmente.

Il BMS comune sarà uno strumento tecnico per facilitare l'identificazione di una persona che può essere registrata in più banche dati. Conserverebbe i modelli dei dati biometrici (impronte digitali e immagini del volto) contenuti nei sistemi di informazione centralizzati dell'UE (vale a dire il SIS, il sistema Eurodac, l'EES, il VIS e il sistema ECRIS-TCN). Permetterebbe, da un lato, di ricercare simultaneamente i dati biometrici conservati nei diversi sistemi e, dall'altro lato, di confrontarli.

IL CIR faciliterebbe l'identificazione delle persone anche nel territorio degli Stati membri e contribuirebbe altresì a semplificare l'accesso delle autorità di contrasto della criminalità a sistemi di informazione estranei al settore del contrasto. Il CIR conserverebbe dati anagrafici e biometrici registrati nel VIS, nel sistema ECRIS-TCN, nell'EES, nel sistema Eurodac e nell'ETIAS. I dati sarebbero conservati, logicamente separati, in base al sistema da cui provengono.

Il MID sarebbe uno strumento che permetterebbe di collegare le identità presenti nel CIR e nel SIS e conserverebbe i collegamenti tra le registrazioni. Conserverebbe i collegamenti che forniscono informazioni laddove una o più corrispondenze definite o possibili siano rilevate o qualora si utilizzi un'identità fraudolenta. Verificherebbe se i dati oggetto dell'interrogazione o i dati di partenza sono presenti in più di uno dei sistemi per individuare identità multiple (vale a dire stessa serie di dati biometrici collegati a dati anagrafici diversi o stessa/analoga serie di dati anagrafici collegati a dati biometrici diversi). Il MID evidenzierebbe le registrazioni di identità anagrafica per le quali esiste un collegamento in sistemi diversi.

Osservazioni generali

Stante i regolamenti, le quattro componenti dell'interoperabilità mirano a fornire agli utenti autorizzati un accesso rapido, continuato, sistematico e controllato ai sistemi di informazione pertinenti, agevolare, nel territorio degli Stati membri, le verifiche di identità dei cittadini di paesi terzi, rilevare le identità multiple collegate alla stessa serie di dati e semplificare l'accesso delle autorità di contrasto a sistemi di informazione estranei al settore del contrasto. Inoltre, istituirebbero un archivio centrale di relazioni e statistiche («CRRS») e il formato universale dei messaggi («UMF») e introdurrebbero meccanismi automatizzati di controllo della qualità dei dati.

Sebbene il progetto dia l'impressione che l'interoperabilità sia la componente finale di sistemi di informazione già interamente funzionanti (o quanto meno di sistemi i cui atti giuridici istitutivi siano già «stabili» e nelle fasi finali del processo legislativo), va sottolineato che ciò non è il caso. Di fatto, come già detto sopra, tre dei sei sistemi di informazione dell'UE che i regolamenti tentano di mettere in interconnessione non sono al momento esistenti (ETIAS, ECRIS-TCN ed EES), due sono attualmente in revisione (SIS ed Eurodac) e uno sarà oggetto di revisione nel corso dell'anno (VIS). Ne consegue che, allo stato attuale, è pressoché impossibile valutare le implicazioni esatte per la protezione della vita privata e dei dati di un sistema così complesso e con così tanti «elementi mobili». Per tali motivi le modalità di salvaguardia dei diritti fondamentali in tale contesto, dovranno essere rivalutate mano a mano che i diversi strumenti giuridici interconnessi progrediranno nel corso dei processi legislativi.
Si può tuttavia già dire che, in termini sia legali sia tecnici, le proposte contenute nei regolamenti aggiungono un ulteriore livello di complessità ai sistemi esistenti nonché a quelli ancora in fase di elaborazione, le cui esatte implicazioni sono difficilmente valutabili in questa fase. Tale complessità avrà implicazioni non solo per la protezione dei dati, ma anche per la governance e la supervisione dei sistemi.

L'Incaricato riconosce che l'interoperabilità, purché attuata in modo ponderato e nel pieno rispetto dei diritti fondamentali, compresi i diritti alla vita privata e alla protezione dei dati, potrebbe rivelarsi uno strumento utile per soddisfare le necessità legittime delle autorità competenti, utilizzando sistemi di informazione su larga scala, e per contribuire allo sviluppo di una condivisione efficace ed efficiente delle informazioni.

Preme tuttavia rilevare che l'interoperabilità non è esclusivamente o prevalentemente una scelta tecnica, ma piuttosto una scelta politica, tale da avere profonde conseguenze giuridiche e sociali, che non possono essere nascoste dietro presunte modifiche tecniche.

La decisione del legislatore dell'UE di realizzare sistemi di informazione su larga scala interoperabili mostra la tendenza a unire la normativa e gli obiettivi politici diversi dell'UE (vale a dire controlli alle frontiere, asilo e immigrazione, cooperazione di polizia e ora anche cooperazione giudiziaria in materia penale) nonché a concedere l'accesso alle banche dati del settore di contrasto della criminalità e di gestione delle frontiere ad autorità estranee a questi settori. Ciò non avrà soltanto conseguenze permanenti e profonde sulla struttura dei sistemi di informazione e sul loro modo di funzionamento, bensì cambierà altresì il modo in cui i principi giuridici in questo settore sono stati tradizionalmente interpretati, segnando pertanto un «punto di non ritorno».

Si può citare come esempio l'uso di ECRIS-TCN. Di fatto, il suo utilizzo a fini di gestione delle frontiere implicherebbe inevitabilmente l'ulteriore trattamento dei dati conservati in ECRIS-TCN per scopi diversi da quelli inizialmente previsti dall'accordo politico su ECRIS-TCN. Infatti, il sistema centrale ETIAS sarebbe in grado di interrogare i dati ECRIS-TCN per verificare se il richiedente ETIAS è una persona i cui dati sono registrati in ECRIS-TCN per reati di terrorismo e altri reati gravi. Questo uso consentirebbe inoltre a una nuova categoria di autorità competenti per la gestione delle frontiere di accedere ai dati personali contenuti nell'ECRIS-TCN. Né il regolamento ETIAS né l'accordo politico sul regolamento ECRIS-TCN (come concordato) prevedono l'uso di ECRIS-TCN ai fini della gestione delle frontiere. L'utilizzo dei dati conservati in ECRIS-TCN per la gestione delle frontiere andrebbe ben oltre le finalità definite per ECRIS-TCN nel suo atto giuridico (nella sua versione attuale). Pertanto non si può ritenere che l'estensione del campo di applicazione di ECRIS-TCN, una banca dati centralizzata contenente informazioni molto sensibili sulle persone, sia un mero adeguamento tecnico. Ciò potrebbe persino essere un esempio di "uso improprio", cioè una graduale espansione dell'uso di un sistema o database al di là dello scopo originario. Facilitare l'accesso delle autorità di contrasto della criminalità e di gestione delle frontiere a sistemi estranei al loro settore, anche se in misura limitata, ha implicazioni tutt'altro che insignificanti in termini

di diritti fondamentali. L'accesso di routine potrebbe, a parer nostro, rappresentare una violazione del principio di limitazione delle finalità.

Conclusione

Benché l'interoperabilità possa essere vista inizialmente soltanto come uno strumento per facilitare l'uso dei sistemi, le proposte introdurrebbero nuove possibilità di accesso e uso dei dati archiviati nei diversi sistemi, al fine di combattere la frode di identità, agevolare i controlli di identità nonché semplificare l'accesso delle autorità di contrasto della criminalità a sistemi di informazione estranei al settore del contrasto. In particolare, le proposte creano una nuova banca dati centralizzata che conterrebbe informazioni su milioni di cittadini di paesi terzi, compresi i loro dati biometrici. In ragione della scala della banca dati e della natura dei dati da conservarvi, le conseguenze di una violazione dei dati potrebbero danneggiare gravemente un numero potenzialmente molto elevato di persone. Qualora tali informazioni cadessero nelle mani sbagliate o fossero utilizzate in modo sbagliato, la banca dati potrebbe diventare uno strumento pericoloso per i diritti fondamentali.

Si teme in particolare che il progetto in questione porti le autorità a credere che, poiché i dati sono già registrati in un sistema, questi possono essere utilizzati regolarmente e con la stessa facilità per scopi diversi rispetto a quelli per i quali sono stati originariamente raccolti, senza esplicita giustificazione o discussione trasparente, malgrado il rischio di un maggiore impatto sulla vita delle persone. In merito si ricorda che il trattamento dei dati, anche se considerato proporzionato ad una finalità specifica, può diventare inadeguato o eccessivo quando gli stessi dati sono ulteriormente trattati per finalità aggiuntive. Inoltre, è importante ricordare che i dati personali relativi alle condanne penali sono considerati più sensibili e soggetti a speciali garanzie previste dalla legislazione sulla protezione dei dati. Pertanto, le estensioni dell'uso dei sistemi di informazione sono possibili unicamente se sono conciliabili con il principio di limitazione delle finalità, uno dei principi fondamentali della legislazione in materia di protezione dei dati. Eccezioni a questo principio sono possibili, ma solo nel rispetto di rigorose condizioni, in particolare che il trattamento dei dati per un'altra finalità sia previsto da una base legale chiara e che ciò sia necessario e proporzionato.

Trattandosi di un'acquis di Schengen le norme in questione vengono recepite senza che vi sia stato un vero e proprio dibattito in merito alla portata del problema che si in-

tende risolvere con l'interoperabilità dei sistemi informatici a livello Svizzero, onde garantire che le misure proposte siano adeguate e proporzionate.

Pertanto è essenziale non solo incorporare garanzie legali e tecniche ma sarà fondamentale accrescere la formazione degli utenti finali in merito al corretto utilizzo dei sistemi a loro disposizione e adottare delle rigorose misure organizzative. È altresì necessario prestare particolare attenzione alla definizione delle finalità della banca dati e delle relative condizioni e modalità d'uso.

L'Incaricato desidera richiamare l'attenzione sull'attuale tendenza a confondere le diverse finalità della migrazione e della gestione delle frontiere, della sicurezza interna e della cooperazione giudiziaria in materia penale. In merito si osserva che, sebbene sia possibile realizzare sinergie tra questi settori, si tratta di settori politici diversi, con obiettivi diversi e attori chiave distinti. Pertanto, l'analisi della necessità e della proporzionalità di cui sopra dovrebbe tener conto anche dei settori d'intervento in cui le misure proposte sarebbero applicate e dei rispettivi ruoli e missioni dei principali attori coinvolti in questi settori.

Si ricorda inoltre che le nuove norme federali e cantonali in materia di protezione dei dati impongono al responsabile del trattamento di effettuare, prima del trattamento, una valutazione d'impatto sulla protezione dei dati per tutte le operazioni di trattamento che possono presentare un rischio elevato per i diritti e le libertà delle persone interessate (conformemente ai principi della protezione dei dati fin dalla fase di progettazione e della protezione dei dati per difetto). Il sistema d'informazione ETIAS e l'ECRIS-TCN comportano l'uso di queste operazioni di trattamento che possono generare un rischio elevato e richiederanno pertanto valutazioni d'impatto sulla protezione dei dati prima del trattamento. Ciò porterà alla definizione di controlli supplementari da attuare o alla modifica dei controlli esistenti sia internamente sia da parte dell'Incaricato.

Rimaniamo a disposizione per ulteriori approfondimenti e le trasmettiamo i nostri cordiali saluti.

Carine Anato